ProSecure™ 统一威胁管理平台

UTM 产品系列



潜藏在网页中的病毒和垃圾邮件、邮件钓鱼攻击、垃圾邮件、携毒邮件等等安全威胁都能够轻而易举地穿透传统防火墙的防御。商用网络是一个经常受到严重影响的群体，并且这个群体不同于大型企业，他们一般都没有足够的时间和资源来巩固和防御他们的网络。再者，这些安全威胁也一直在发展变化着：较早前，针对商用网络的安全威胁很大部分被称为“注入式”威胁，由黑客来向目标企业进行攻击——但是这种攻击很少在大型企业发生。但是，随着Web 2.0和云计算技术的快速发展，攻击的特征已经向“拖挂式”转变。当用户使用Web 2.0和云计算技术的时候，他们也将安全威胁一起带到网络的内部。

由于全面的网络安全解决方案需要有强大的处理能力来实时地检查网络流量，现行的大部分一体式网络安全解决方案一般使用初级的安全检验技术来换取全面的速度，而真正的安全需要同时满足速度和覆盖率两者的需求。

全球成长型商用网络专家和 Internet 应用安全厂商美国网件公司（NETGEAR）推出其最新的统一威胁管理产品，为商业网络提供企业级的全面安全解决方案。NETGEAR ProSecure™ UTM 统一威胁管理网关系列产品在 NETGEAR 的 **SPI 防火墙**和 **VPN 技术** (IPSec VPN 和 SSL VPN)的基础上，引入 NETGEAR 专利的串流扫描技术，再融合了企业级的**防病毒**（Anti-Virus）、**Web 内容过滤**（Web-Filter）、**反垃圾邮件**（Anti-Spam）、 **入侵检测**（IPS）以及**应用程序控制**（Appliacation Control）等功能。主要针对来源于互联网的安全威胁，包括恶意软件、间谍软件、蠕虫病毒、垃圾邮件、网络钓鱼攻击等攻击进行有效防范，对进出的所有流量进行扫描分析，确保所有威胁和病毒在进入网络之前就被检测和处理。

NETGEAR ProSecure™ UTM关键特性

• **优秀的恶意软件防护引擎：**ProSecure™ UTM 产品包含了企业级的恶意软件防护引擎，比传统的商用网络一体化 UTM 设备高 200 倍的覆盖率，可检测超过 130 多万的威胁。特征库可在每小时自动更新，无需人工干预。

• **NETGEAR 专利的串流扫描技术：**基于 NETGEAR 专利的串流扫描技术，数据流在一进入网络被开始进行扫描分析，实现 Web 流量扫描的超低延时。

• **垃圾邮件云分析体系：**ProSecure™ UTM 产品采用混合的云分析架构，从超过 5000 万个数据源中收集安全威胁的数据，在几分钟内便可分类检测出新的垃圾邮件，不需要学习期，

不需要额外的操作。由于云分布分析体系的应用，也将误杀率降到最低，并且适用于任何类型的垃圾邮件。

• **云分布 Web 分析与 URL 过滤技术：**采用了新一代混合云分布 URL 过滤技术，包含了上亿个被分类的 URL 条目。新的网站分类可实时加入到数据库中。目前的数据库涵盖了高达 64 个分类内容。在设置过程中可基于用户与组进行灵活过滤。

• **零时差威胁保护：**采用了启发式智能检测机制来快速检测未知的安全威胁，防止网络暴露在新的未分类安全威胁之下。

• **NETGEAR 入侵防御系统：**采用策略驱动语言来防止黑客对网络进行渗透。

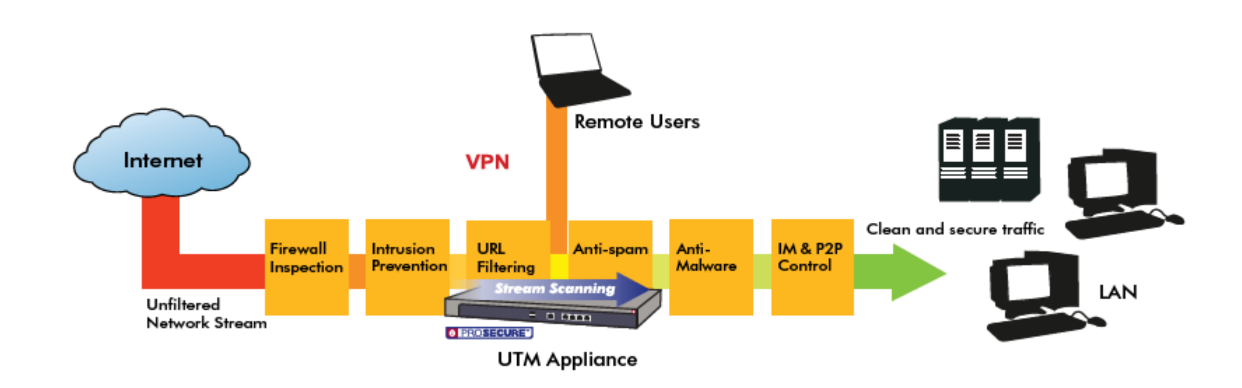
• **IM 和 P2P 程序控制：**ProSecure™ UTM 可禁止使用公共的 IM 客户端软件与点对点（P2P）客户端软件，从而帮助企业节省带宽，提高生产率。

• **SSL & IPsec VPN 远程访问：**支持 SSL VPN，无需客户端软件。用户可以随时、随地自由登陆到企业内部网络。也同时支持 IPsec VPN，使用点对点安全隧道，方便客户端的远程访问。VPN 功能均无需额外购买授权许可便可实现。

• **内嵌的 VPN/Firewall：**具有双千兆广域网接口*，并提供了负载均衡和 failover 功能。具备 4 个千兆局域网接口，1 个 DMZ 接口。带有防火墙高级状态包检测功能 （SPI）功能，能够对拒绝服务 （DoS） 进行有效防御。

保证性能的全面网络安全

NETGEAR ProSecure™统一威胁管理（UTM）平台将性能和全面的安全性融为一体。基于专利的串流扫描技术，NETGEAR能够使用广泛全面的恶意软件数据库，并且同时保证了高吞吐量和低时延。灵活的软件模块化架构使得串流扫描技术在扫描文件和数据流的时候比常规的扫描技术快5倍！借助这个架构的优势，ProSecure™ UTM产品采用了来自于NETGEAR和Sophos™的数十万的恶意软件特征库——相比同类用于商用网络的产品高了200倍的覆盖率。同时，在此架构上整合了最优秀的云分布Web过滤技术和垃圾邮件云分布分析技术，再加上NETGEAR的防火墙及VPN功能，共同打造了为商用网络服务的网关安全解决方案。

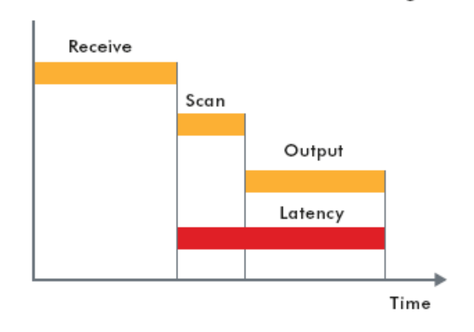


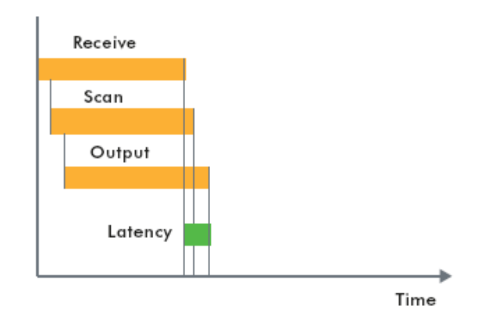
专利的串流扫描技术

由于 Web 流量对延时相当敏感，扫描技术也就相应地需要有极高的性能。因此，要将企业级的高级安全软件技术整合到商业网络的一体化平台是一项非常艰难的挑战。基于以上原因，NETGEAR ProSecure™ UTM 引入了 NETGEAR 专利的串流扫描技术，可以当数据

流进入网络时便开始进行分析。NETGEAR 串流扫描技术比传统的先缓存整个文件再进行扫描的批量扫描技术提高了数倍的效率。

由于批量扫描技术的特性，网络往往会增加延时。虽然延时对于 Email 流量来说并非不可接受，但是对于大量的 HTTP Web 流量，延时会使得网页浏览缓慢到令人难以接受。过去的一体化解决方案经常通过减少恶意代码特征库、只扫描部分文件类型、或者避免同时扫描所有 Web 流量等方式来降低延时。但是这种方法会将整个网络暴露给恶意软件攻击。





简安装，易管理

NETGEAR ProSecure™ UTM可以简便地替代掉任何现有的防火墙或路由器。10个步骤的简单设置向导可引导用户在几分钟内将UTM成功安装并正常运行。UTM通过基于Web的页面进行直观的管理。通过管理界面来设置定时的策略和警报、查询统计信息和图形报表、深入到IP地址层的数据、整合日志信息与网络管理的SNMP等。恶意软件和IPS的特征库、软件、固件等的等级将可通过UTM在线自动完成。

对很多管理员来说，管理一个个单一的许可证向来是最大的烦恼。在计算机、员工数量上升的时候另行购买额外的许可证既浪费时间又增加开销。NETGEAR STM 系列产品直接提供 Web 和 Email 的保护服务许可证而不对“每用户”进行单独授权。

ProSecure™ UTM 统一威胁管理产品系列对照

产品型号	UTM10	UTM25
规模参考		
用户类型	小型网络	小型网络
建议并发用户数	1-15	10-30
防病毒吞吐量	31 Mbps	45 Mbps
SPI 防火墙吞吐量	133 Mbps	153 Mbps
IPS 吞吐量	TBD	TBD
VPN 吞吐量	TBD	TBD
并发连接数	8,000	20,000
VLAN 数量	4,096	4,096
内容安全		
Web （HTTP, HTTPS, FTP）	●	●
Email （SMTP, POP3, IMAP）	●	●
串流扫描	●	●
进出双向检测	●	●
入侵检测 / 防御	●	●
零时差保护	●	●
恶意软件特征库	600,000	600,000
特征库自动更新	每小时	每小时
HTTPS 扫描与过滤	●	●
Web 内容过滤	根据 HTML 文件体关键字和文件扩展名进行过滤	
Web 对象过滤	ActiveX, Java™, Flash, JavaScript™, Proxy, Cookies	
Email 内容过滤	根据标题关键字、加密附件、文件扩展名文件名进行过滤	
垃圾邮件云分布体系	●	●
防垃圾邮件实时黑名单 （RBL）	●	●
用户自定义垃圾邮件允许/禁止列表	根据发件人邮件地址、域名、IP 地址，收件人邮件地址、域名进行过滤	
云分布 Web 分类（64 个分类）	●	●
即时通信程序 （IM） 控制	MSN® Messenger, Yahoo!® Messenger, Skype, mIRC, Google Talk	
点对点程序 （P2P） 控制	BitTorrent™, eDonkey, Gnutella	
最大用户数	无限制	
防火墙特性		
状态包检测 （SPI）	端口/服务禁止、拒绝服务防御（DoS）、Stealth 模式、禁止 TCP 泛洪 / UDP 泛洪、WAN / LAN 的 Ping 应答控制	
广域网模式	NAT, 路由	
ISP 地址指派方式	DHCP, 静态 IP 地址指定, PPPoE, PPTP	
NAT 模式	1-1 NAT, PAT	

路由协议	静态路由，动态路由，RIPv1, RIPv2	
VoIP	SIP ALG	
DDNS	DynDNS.org, TZO.com, Oray.net	
防火墙功能	端口转发、端口触发、DNS 代理、MAC 地址克隆/欺骗、网络时间协议（NTP）、诊断工具（ping, DNS lookup, trace route,其它）、自动上连，线序自适应，第 3 层质量服务 （QoS）、LAN-to-WAN 和 WAN-to-LAN （ToS）	
DHCP	DHCP 服务器、DHCP 中继	
用户认证	活动目录, LDAP, Radius, 本地用户数据库	
PCI Compliance Two Factor 认证	●	●
VPN		
点对点 VPN 隧道	10	25
远程接入 SSL VPN	5	13
IPsec 加密算法	DES, 3DES, AES（128,192,256 bit）	
IPsec 认证算法	SHA-1, MD5	
密钥交换方式	IKE, Manual Key, Pre-Shared Key, PKI, X.500	
IPsec NAT 穿透	●	●
SSL 版本支持	SSLv3, TLS1.0	
SSL 加密支持	DES, 3DES, ARC4, AES（128,256 bit）	
SSL 消息完整性验证	MD5, SHA-1, MAC-MD5/SHA-1, HMAC-MD5/SHA-1	
SSL 证书支持	RSA, Diffie-Hellman, Self	
SSL VPN 平台支持	Windows 2000 / XP / Vista®, Mac® OS X 10.4+	
部署		
VLAN 支持	●	●
双广域网接口 Fail-over		●
智能流量负载均衡（基于流量字节计数）		●
配置智能向导	设备安装、IPsec VPN、SSL VPN	
日志与报表		
管理	HTTP/HTTPS, SNMP v2c	
报表	信息统计、图形报表、自动爆发警报、自动恶意软件通知、系统通知	
日志	流量、恶意软件、垃圾邮件、内容过滤、邮件过滤、系统、服务、IPS、端口扫描、IM、P2P、防火墙、IPsec VPN、SSL VPN	
日志发送	管理界面查询、Email 发送、Syslog	
硬件		
WAN Gigabit RJ45 端口	1	2
LAN Gigabit RJ45 端口	4	4
DMZ 接口 （可配置）	1	1
管理控制台接口	RS232	RS232

USB 接口	1	1
主要服从规范	FCC Class A, CE, WEEE, RoHS	
保存及运行温度	运行温度 0°-45° C （32°-113° F） 保存温度 -20°-70° C （-4°-158° F）	
湿度	运行 最大相对湿度 90%，保存 最大相对湿度 95%	
电气规范	100-240V, AC/50-60Hz, Universal Input, 1.2 Amp Max	
尺寸 （长 x 高 x 深） 厘米	33 x 4.3 x 20.9	33 x 4.3 x 20.9
尺寸 （长 x 高 x 深） 英寸	13 x 1.7 x 8.2	13 x 1.7 x 8.2
重量 千克	2.1	2.1
重量 磅	4.6	4.6
包装内容	ProSecure™ 平台 （UTM10 或 UTM25）、以太网线、电源线、上架配件、质保卡，快速安装指南、授权许可证 （仅供套件）	
硬件质保	1 年	

ProSecure™ UTM 统一威胁管理产品订购信息

订购信息		
硬件 （仅防火墙与 VPN 功能）		
UTM10-100AJS	UTM25-100AJS	
组合套装 （硬件，包括 1 年的 Web 和 Email 功能，1 年的软件维护与升级和技术支持）		
UTM10EW-100AJS	UTM25EW-100AJS	
1 年授权许可		
Web 威胁管理	Email 威胁管理	软件维护、升级与技术支持
UTM10W-10000S	UTM10E-10000S	UTM10M-10000S
UTM25W-10000S	UTM25E-10000S	UTM25M-10000S
3 年授权许可		
Web 威胁管理	Email 威胁管理	软件维护、升级与技术支持
UTM10W3-10000S	UTM10E3-10000S	UTM10M3-10000S
UTM25W3-10000S	UTM25E3-10000S	UTM25M3-10000S